Carbon Black App Control

Positive security model allows only trusted software to run

Use cases

- Lock down systems on-premises or in private or public clouds
- Secure fixed-function devices
- Protect end-of-life (EOL) operating systems
- Secure air-gapped systems

Benefits

- Stop malware, ransomware and next-gen attacks
- Reduce unplanned downtime of critical systems
- Consolidate endpoint agents
- Prevent unwanted change to system configuration
- Meet IT risk and audit controls across major regulatory mandates
- Increase efficiency of IT resources with streamlined IT audit processes
- Protect legacy systems running on EOL operating systems
- Identify all software in critical environments
- Prevent writing data to unsanctioned devices

As security threats and malware evolve, so too has the need for technologies to combat these threats. Organizations can't afford the loss of productivity caused by unscheduled downtime or performance degradation associated with a security breach. Neither can they afford the loss of reputation and costs. Given this rapidly evolving landscape, the question remains: What is the best way to protect against an ever-increasing, and more targeted, number of threats to servers and endpoints?

There are two approaches to security: positive and negative. Negative security, or the ability to detect and thwart known-bad events, has provided a layer of security assurance for years. The ability to block known viruses, worms and other bad event signatures has kept many systems from being compromised. However, new attacks have evolved that are outside the scope of the negative security model. The negative security model isn't bad; in fact, it's essential. But it isn't enough.

A positive security model identifies software with a known degree of trust, only allowing access to trusted resources. The positive model assumes that unknown software is not to be trusted and requires that trust be assigned before granting access and usage. The classic positive security model only delivers known-good requests and results.

Carbon Black® App Control™ employs a positive security model to protect critical systems on-premises or in private or public cloud. This prevents unwanted changes and ensures continuous compliance with regulatory mandates.

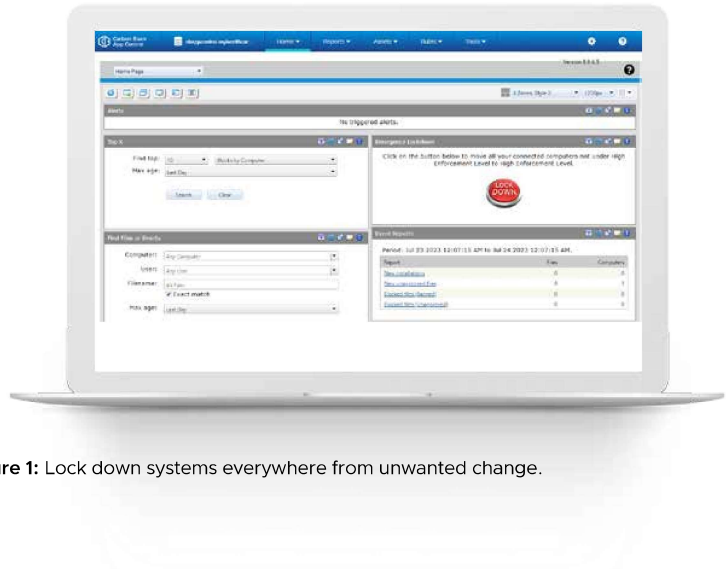

Figure 1: Lock down systems everywhere from unwanted change.

Features

- Application control
- File integrity monitoring and control
- Device control
- Memory protection
- Registry protection
- Application catalog inventory
- Common platform enumeration
- Rapid configurations
- Content-based inspection
- Process hollowing protection

Platforms

Sensor support:

- Windows XP, Server, Embedded, POS
- Mac OS X
- RHEL Linux
- Oracle RHCK Linux

Holistic approach to positive security

Carbon Black App Control takes a holistic approach to positive security by including the following:

- Application control (allowlisting and denylisting) offers varying degrees of control over what an application can do as it interacts with system resources.
- File integrity monitoring (FIM) examines the integrity of sensitive files, registry keys and folders within the host operating system and checks whether files have been altered or compromised. File integrity control (FIC) can report or block changes.
- Device control provides full control to define or restrict data transfer from external storage media, such as USB devices. By implementing a set of access rules, organizations can set parameters to grant or restrict connection from specific devices, users or groups at scheduled times.
- Memory protection controls memory access rights. The main purpose of memory protection is to prevent a process from accessing memory that has not been allocated to it.
- Registry protection prevents system-critical registry keys on Windows from being modified. It is essential to protect registry keys against attack because irreversible damage can be caused if important keys are corrupted or modified. Carbon Black App Control can report or block changes.

Flexible deployment

As IT and security deployments migrate to the cloud, security gaps can be created unless attention remains on these now vulnerable areas. Paradoxically, many companies continue to maintain critical systems and data on air-gapped servers or on systems running end-of-life operating systems. Carbon Black App Control offers a positive security approach whether in a data center or on Amazon Web Services (AWS), Microsoft Azure, or hosted private clouds. A cloud-only approach to security does not protect:

- Air-gapped systems disconnected from the internet and the Carbon Black App Control server
- Fixed-function devices, such as ATMs, point-of-sale systems, kiosks, and medical devices
- EOL operating systems, such as Windows XP and Windows Server 2003 and 2008
- Critical systems that are the lifeblood of the company using proprietary software and data

Trusted content approval

Carbon Black App Control does not rely on a library or list of files to maintain, which can easily become outdated. Instead, Carbon Black App Control employs a trust-based approach to content approval, comprised of multiple mechanisms that allow file approval without having to maintain a list of hashes to approve. This makes a positive security posture easier to achieve. These include:

- IT and cloud-driven trust – Provide trusted directories and threat/reputation from the cloud.
- Trusted publishers – Allow organizations to choose to trust Google, Adobe, or other sources they trust.
- Custom rules – Provide more granular control, allowing files to be approved by path, process and users.
- External sources – Send new/unknown files for static or dynamic analysis, then approve or ban based on the result using the events rules feature.

Summary

Carbon Black App Control can lock down your environment, prevent unwanted changes, and ensure continuous compliance with regulatory mandates. Employing a positive security model, which enables a default/deny security posture, Carbon Black App Control continuously protects against cyberthreats that evade traditional security defenses.

Carbon Black App Control does not rely on a library or list of files to maintain, which can easily become outdated. Instead, it employs multiple approval methods, including IT and cloud-driven trust, trusted publishers, custom rules, and validated external sources.

Carbon Black App Control provides peace of mind.